arXiv:math/0101242v1 [math.NT] 29 Jan 2001

ON A CHARACTER SUM PROBLEM OF H. COHN

PÄR KURLBERG

ABSTRACT. Let f be a complex valued function on a finite field F such that $f(0) = 0$, $f(1) = 1$, and $|f(x)| = 1$ for $x \neq 0$. Cohn asked if it follows that f is a nontrivial multiplicative character provided that $\sum_{x \in F} f(x)\overline{f(x+h)} = -1$ for $h \neq 0$. We prove that this is the case for finite fields of prime cardinality under the assumption that the nonzero values of f are roots of unity.

1. INTRODUCTION

Let p be prime and let F_{p^k} be the finite field with p^k elements. Let $f : F_{p^k}^{\times} \to \mathbf{C}$ be a nontrivial multiplicative character, and extend f to a function on F_{p^k} by letting $f(0) = 0$. It is then easy to see that the following holds:

$$\sum_{x \in F_{p^k}} f(x)\overline{f(x+h)} = \begin{cases} -1 & \text{if } h \neq 0 \\ p^k - 1 & \text{if } h = 0 \end{cases} \tag{1.1}$$

Cohn asked (see p. 202 in [3]) if the converse is true in the following sense: if a function $f : F_{p^k} \to \mathbf{C}$ satisfies

$$f(0) = 0, \;\; f(1) = 1, \;\text{ and } |f(x)| = 1 \text{ for } x \neq 0 \tag{1.2}$$

and equation 1.1, does it follow that f is a multiplicative character?

The problem has recently received some attention. In [2], Choi and Siu proved that the converse is not true for $k > 1$. One of the arguments given is quite pretty, and proceeds as follows: Let λ be a linear automorphism of F_{p^k} so that $\lambda(1) = 1$. If f satisfies 1.1 and 1.2, so does f composed with λ. Now, if f is an injective multiplicative character then the converse being true implies that f composed with λ must be an injective multiplicative character. On the other hand, a simple counting argument shows that the number of possible λ's is greater than the number of injective characters.

However, the case $k = 1$ remains unresolved. In [1], Biro proved that there are only finitely many functions satisfying equation 1.1 and 1.2

Author supported in part by the National Science Foundation (DMS 0071503).

for each p. Biro also solved the following "characteristic p" version of the problem ([1], Theorem 2):

Theorem (Biro)**.** *Let p be a prime, let F_p be the finite field with p elements, and $F \supset F_p$ any field of characteristic p. Assume that there is given an $a_i \in F$ for every $i \in F_p$ such that $a_0 = 0, a_1 = 1, a_i \neq 0$ for $i \neq 0$, and*

$$\sum_{i \in F_p^\times} \frac{a_{i+j}}{a_i} = -1$$

for every $j \in F_p^\times$. Then $a_i = i^A$ for every $i \in F_p$ with some $1 \leq A \leq p-2$.

Using this Biro deduces that the converse holds for functions taking values in $\{-1, 0, 1\}$.[1] In fact, if m is coprime to p, then the case of the nonzero values of f being m-th roots of unity can be deduced in a similar way: Let $\mathfrak{O}$ be the ring of integers in $\mathbf{Q}(e^{2\pi i/m})$, and let $\mathfrak{P} \subset \mathfrak{O}$ be a prime ideal lying above p. The result then follows from the theorem by letting $F = \mathfrak{O}/\mathfrak{P}$ and noting that m-th roots of unity are distinct modulo p. (Since $|f(x)| = 1$ for $x \neq 0$ we have $\overline{f(x)} = 1/f(x)$.)

The aim of this paper is to show that the converse is true for the case $k = 1$, under the additional assumption that the nonzero values of $f : F_p \to \mathbf{C}$ are m-th roots of unity, including the case $p|m$. We begin by giving a proof that does not depend on Biro's result for the case $(m, p) = 1$, and we then show how to modify the argument for the general case.

Acknowledgements: I would like to thank Ernest Croot, Andrew Granville, Robert Rumely, and Mark Watkins for helpful and stimulating discussions. I would also like to thank the referee for several suggestions on how to improve the exposition, and for pointing out that the case $p|m$ can be deduced independently of Biro's theorem.

2. Preliminaries

In what follows we assume that p is odd since the case $p = 2$ is trivial.

We will use the following conventions: if a function f takes values in $\mathbf{C}$ and $\sigma \in \mathrm{Aut}(\mathbf{C}/\mathbf{Q})$, then we let f^σ be the function defined by $f^\sigma(x) = \sigma(f(x))$. We regard $\psi(x) = e^{2\pi i x/p}$ as a nontrivial additive character of F_p. For an integer t, ψ_t will denote the character $\psi_t(x) = \psi(tx)$. By ζ_m we denote the m-th root of unity $\zeta_m = e^{2\pi i/m}$.

[1]There appears to be several independent proofs of this result, see the introduction in [2].

Let m be even and large enough so that all nonzero values of f are m-th roots of unity, and write $m = np^k$, where $(n,p) = 1$. Let $K = \mathbf{Q}(\zeta_n)$, $L = K(\zeta_p, \zeta_{p^k})$, and let $G = \mathrm{Gal}(L/\mathbf{Q})$, $H = \mathrm{Gal}(L/K)$ denote the Galois groups of $L/\mathbf{Q}$ and L/K. By $\mathfrak{O}_K$ and $\mathfrak{O}_L$ we will denote the ring of integers in K respectively L.

The "Gauss sum"

$$G(f,\psi) = \sum_{x=0}^{p-1} f(x)\psi(x)$$

is clearly an algebraic integer. As in the case of classical Gauss sums, the absolute value of $G(f,\psi)$ can easily be determined:

Lemma 1. *If f satisfies 1.1, then*

$$|G(f,\psi_t)| = \begin{cases} \sqrt{p} & \textit{if } t \not\equiv 0 \mod p, \\ 0 & \textit{if } t \equiv 0 \mod p. \end{cases}$$

Proof. We have

$$\begin{aligned} |G(f,\psi_t)|^2 &= \sum_{x,y\in F_p} f(x)\overline{f(y)}\psi(t(x-y)) = \sum_{x,h\in F_p} f(x)\overline{f(x+h)}\psi(-th) \\ &= \psi(0)\sum_{x\in F_p} f(x)\overline{f(x)} + \sum_{h\in F_p^\times}\psi(-th)\sum_{x\in F_p} f(x)\overline{f(x+h)} \\ &= p-1-\sum_{h\in F_p^\times}\psi(-th) = \begin{cases} p & \text{if } t \not\equiv 0 \mod p, \\ 0 & \text{if } t\equiv 0 \mod p, \end{cases} \end{aligned}$$

□

The action of complex conjugation on K is given by an element in G, and since G is abelian, equation 1.1 is G-invariant. I.e., if f satisfies 1.2, so does f^σ for all $\sigma \in G$. But if $\sigma \in G$ then $\sigma(G(f,\psi)) = G(f^\sigma, \psi_t)$, where $\sigma(\zeta_p) = \zeta_p^t$. Since f^σ also satisfies 1.1, we find that $|G(f^\sigma,\psi_t)| = p^{1/2}$, and hence the $\mathbf{Q}$-norm of $G(f,\psi)$ is a power of p. The factorization of the principal ideal $G(f,\psi)\mathfrak{O}_L$ thus consists only of prime ideals $\mathfrak{P}_L|p$.

It is well known that $\mathbf{Q}(\zeta_{p^k})/\mathbf{Q}$ is totally ramified over p, and that $\mathbf{Q}(\zeta_n)/\mathbf{Q}$ does not ramify at p if $(n,p) = 1$. Comparing ramification indices gives that if $\mathfrak{P}_K$ is a prime ideal in $\mathfrak{O}_K$ that divides p, then $\mathfrak{P}_K$ is totally ramified in L. In particular, if $\mathfrak{P}_L$ is any prime ideal in the ring of integers in $\mathfrak{O}_L$ that lies above p, then $\sigma(\mathfrak{P}_L) = \mathfrak{P}_L$ for all $\sigma \in H$.

Let $l = \max(1,k)$. Then H consists of elements σ_t such that

$$\sigma_t(\zeta_{p^l}) = \zeta_{p^l}^t, \quad \sigma_t(\zeta_n) = \zeta_n.$$

Choose t so that σ_t generates H. Applying σ_t to the principal ideal

$$G(f,\psi)\mathfrak{O}_L = \prod_{\mathfrak{P}_L|p} \mathfrak{P}_L{}^{\eta(\mathfrak{P}_L)}$$

we find that

$$\sigma_t(G(f,\psi)\mathfrak{O}_L) = \sigma_t(\prod_{\mathfrak{P}_L|p} \mathfrak{P}_L{}^{\eta(\mathfrak{P}_L)}) = \prod_{\mathfrak{P}_L|p} \mathfrak{P}_L{}^{\eta(\mathfrak{P}_L)} = G(f,\psi)\mathfrak{O}_L$$

and hence $\sigma_t(G(f,\psi)) = uG(f,\psi)$ for some unit u.

Since the absolute value of any complex embedding of $G(f,\psi)$ equals $\sqrt{p}$, we find that all conjugates of $u = \sigma(G(f,\psi))/G(f,\psi)$ has absolute value one. Hence u is in fact a root of unity, and there are integers a, b such that

$$\sigma_t(G(f,\psi)) = \zeta_{p^l}^a \zeta_n^b G(f,\psi). \tag{2.1}$$

3. The case $(m,p) = 1$

Since f is fixed by H we find that $\sigma_t(G(f,\psi)) = G(f,\psi_t)$, and equation 2.1 can, after the change of variable $x \to t^{-1}x$, be written as

$$\sum_{x=1}^{p-1} f(x)\psi(x) = \zeta_p^{-a}\zeta_n^{-b} \sum_{x=1}^{p-1} f(t^{-1}x)\psi(x). \tag{3.1}$$

Lemma 2. *If f takes values in n-th roots of unity for $x \not\equiv 0 \mod p$ and equation 3.1 holds then $a \equiv 0 \mod p$.*

Proof. From 3.1 we obtain that

$$\sum_{i=1}^{p-1} A_i \zeta_p^i = \sum_{i=0}^{p-1} B_i \zeta_p^i \tag{3.2}$$

where $A_i = f(i)$ and $B_i = \zeta_n^{-b} f(t^{-1}(i+a))$. (Note that $B_{p-a} = 0$.) Since $1 = -\sum_{i=1}^{p-1} \zeta_p^i$ we may rewrite 3.2 as

$$\sum_{i=1}^{p-1} A_i \zeta_p^i = \sum_{i=1}^{p-1} (B_i - B_0)\zeta_p^i. \tag{3.3}$$

The elements $\{\zeta_p, \zeta_p^2, \zeta_p^3, \ldots \zeta_p^{p-1}\}$ are linearly independent over K, hence $A_i = B_i - B_0$. From lemma 1 we have $\sum_{x=0}^{p-1} f(x) = 0$, which implies that $\sum_{i=1}^{p-1} A_i = 0$, as well as $\sum_{i=0}^{p-1} B_i = 0$. Therefore,

$$0 = \sum_{i=1}^{p-1} A_i = \sum_{i=1}^{p-1} (B_i - B_0) = \sum_{i=0}^{p-1} B_i - pB_0 = -pB_0.$$

But $B_0 = \zeta_n^{-b} f(t^{-1}(0+a))$ which is nonzero unless $a \equiv 0 \mod p$. $\square$

Thus

$$\sum_{x=1}^{p-1} f(x)\psi(x) = \zeta_n^{-b} \sum_{x=1}^{p-1} f(t^{-1}x)\psi(x) \tag{3.4}$$

and the linear independence of $\{\zeta_p, \zeta_p^2, \zeta_p^3, \dots \zeta_p^{p-1}\}$ over K implies that

$$f(t^{-1}x) = f(x)\zeta_n^b$$

for all $x \neq 0$. Thus

$$f(t^{-k}) = f(t^{-(k-1)})\zeta_n^b = \dots = f(1)\zeta_n^{kb} = \zeta_n^{kb}.$$

Taking $k = p-1$ we find that ζ_n^b is a $(p-1)$-th root of unity, and that f is a multiplicative character.

4. The general case

In this case $m = np^k$ where $(n, p) = 1$ and $k > 0$. We will need the following:

Lemma 3. *If $a_i \in K$ and $\sum_{i=0}^{p^k-1} a_i \zeta_{p^k}^i \in K(\zeta_p)$ then*

$$\sum_{i=0}^{p^k-1} a_i \zeta_{p^k}^i = \sum_{j=0}^{p-1} a_{p^{k-1}j} \zeta_p^j \tag{4.1}$$

Proof. We may assume that $k > 1$. The minimal polynomial for ζ_{p^k} (over K as well as over $\mathbf{Q}$) is given by

$$\frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \dots + x^{(p-1)p^{k-1}}.$$

Hence, by letting $\tilde{i} \in [0, p^{k-1} - 1]$ be a representative of i modulo p^{k-1}, we can rewrite the left hand side of equation 4.1 as

$$\sum_{i=0}^{(p-1)p^{k-1}-1} (a_i - a_{(p-1)p^{k-1}+\tilde{i}})\zeta_{p^k}^i$$

with no further relations among the $\zeta_{p^k}^i$'s, and thus

$$\sum_{i=0}^{(p-1)p^{k-1}-1} (a_i - a_{(p-1)p^{k-1}+\tilde{i}})\zeta_{p^k}^i \in K(\zeta_p)$$

if and only if $a_i - a_{(p-1)p^{k-1}+\tilde{i}} = 0$ for all i not congruent to zero modulo p^{k-1}. $\square$

Recall from equation 2.1 (note that $l = k$ since $k \geq 1$) that

$$\sigma_t(G(f,\psi)) = \zeta_{p^k}^a \zeta_n^b G(f,\psi).$$

Let $\tilde{G} = \zeta_{p^k}^s G(f,\psi)$ where $\sigma_t(\zeta_{p^k}^s)/\zeta_{p^k}^s = \zeta_{p^k}^{-a}$. (Such an s exists as $\sigma_t(\zeta_{p^k}^s)/\zeta_{p^k}^s = \zeta_{p^k}^{(t-1)s}$, and $t \not\equiv 1 \mod p$ since σ_t generates H.) We then have

$$\sigma_t(\tilde{G}) = \sigma_t(\zeta_{p^k}^s G(f,\psi))$$
$$= \sigma_t(\zeta_{p^k}^s)\sigma_t(G(f,\psi)) = \sigma_t(\zeta_{p^k}^s)\zeta_{p^k}^a \zeta_n^b G(f,\psi)) = \zeta_n^b \tilde{G}.$$

The following lemma shows that $\tilde{G}$ must transform by a nontrivial n-th root of unity:

Lemma 4. *There is no integer s such that $\zeta_{p^k}^s G(f,\psi) \in K$.*

Proof. We first assume that $\zeta_{p^k}^s = 1$. Let $G(f,\psi)\mathfrak{O}_L = \prod_{\mathfrak{P}_L|p} {\mathfrak{P}_L}^{\eta(\mathfrak{P}_L)}$ be the factorization of the principal ideal $G(f,\psi)\mathfrak{O}_L$. Since p does not ramify in K, we have $p\mathfrak{O}_K = \prod_{\mathfrak{P}_K|p} \mathfrak{P}_K$, and hence $p\mathfrak{O}_L = \prod_{\mathfrak{P}_L|p} {\mathfrak{P}_L}^e$ where e is the ramification index of $\mathfrak{P}_K$ in L.

Since $\psi(x) = \zeta_p^x$ is congruent to 1 modulo $\mathfrak{P}_L$ for all x, we find that

$$G(f,\psi) = \sum_{x=0}^{p-1} f(x)\psi(x) \equiv \sum_{x=1}^{p-1} f(x) \mod \mathfrak{P}_L$$

for all $\mathfrak{P}_L|p$. Now, since $f(0) = 0$, we have $\sum_{x=1}^{p-1} f(x) = G(f,\psi_0)$ and by lemma 1, $G(f,\psi_0) = 0$. Thus $G(f,\psi) \in \mathfrak{P}_L$ for all $\mathfrak{P}_L|p$, i.e., $\eta(\mathfrak{P}_L) > 0$ for all $\mathfrak{P}_L|p$. But if $G(f,\psi) \in K$ then $e|\eta(\mathfrak{P}_L)$ for all $\mathfrak{P}_L|p$, and since complex conjugation permutes the set of primes of $\mathfrak{O}_L$ that lies above p, and

$$p = G(f,\psi)\overline{G(f,\psi)},$$

we get that ${\mathfrak{P}_L}^{2e}|p\mathfrak{O}_L$ for all $\mathfrak{P}_L$, contradicting that the ramification index is e.

For the general case, the previous argument carries through by noting that $\zeta_{p^k}^s$ is a unit (and thus multiplication of $G(f,\psi)$ by $\zeta_{p^k}^s$ does not change the ideal factorization) and that $G(f,\psi) \in \mathfrak{P}_L$ if and only if $\zeta_{p^k} G(f,\psi) \in \mathfrak{P}_L$. $\square$

Since σ_t has order $p^{k-1}(p-1)$ and $(n,p) = 1$ we find that ζ_n^b must be a nontrivial $(p-1)$-th root of unity. Hence there exists a nontrivial multiplicative character χ of $F_p^\times$ such that $\chi(t^{-1}) = \zeta_n^b$. But $\sigma_t(G(\chi,\psi)) = G(\chi,\psi_t) = \chi(t^{-1})G(\chi,\psi)$ and thus

$$\delta = \frac{\tilde{G}}{G(\chi,\psi)}$$

is σ_t-invariant and hence an element of K. Moreover, $|\delta| = 1$ (for all complex embeddings) since $|\tilde{G}| = |G(\chi, \psi)| = p^{1/2}$.

Write $f(x) = f_1(x)f_2(x)$ where $f_1(x)$ takes values in p^k-th roots of unity and $f_2(x)$ takes values in n-th roots of unity. We will show that $f_1(x)$ must be constant.

Lemma 5. *Let*

$$a_i = \sum_{x:\zeta_{p^k}^s f_1(x)\psi(x)=\zeta_{p^k}^i} f_2(x)$$

If

$$\zeta_{p^k}^s \sum_{x=1}^{p-1} f(x)\psi(x) = \delta \sum_{x=1}^{p-1} \chi(x)\psi(x), \tag{4.2}$$

then $|a_i| = 0$ unless $i = p^{k-1}j$ for $j = 1, 2, \ldots, p-1$, in which case $|a_i| = 1$. In particular, $\zeta_{p^k}^s f_1(x)\psi(x)$ ranges over all nontrivial p-th roots of unity.

Proof. Collecting terms in 4.2 according to the values of $\zeta_{p^k}^s f_1(x)\psi(x)$, we obtain

$$\sum_{i=0}^{p^k-1} a_i \zeta_{p^k}^i = \delta \sum_{i=1}^{p-1} \chi(i)\zeta_p^i \in K(\zeta_p). \tag{4.3}$$

Clearly $a_i \in K$ and $a_i \neq 0$ for at most $p-1$ values of i. Letting $A_i = a_{p^{k-1}i}$ we may, by lemma 3, write equation 4.3 as

$$\sum_{i=0}^{p-1} A_i \zeta_p^i = \delta \sum_{i=1}^{p-1} \chi(i)\zeta_p^i.$$

Since $1 = -\sum_{i=1}^{p-1} \zeta_p^i$ we get that

$$\sum_{i=1}^{p-1} (A_i - A_0)\zeta_p^i = \sum_{i=0}^{p-1} A_i \zeta_p^i = \delta \sum_{i=1}^{p-1} \chi(i)\zeta_p^i$$

and hence $A_i - A_0 = \delta\chi(i)$ for all i.

Since $a_i \neq 0$ for at most $p-1$ values of i, $A_0 \neq 0$ implies that $A_j = 0$ for some $j \neq 0$, and thus $|A_0| = |\delta\chi(j) - A_j| = 1$. Since

$$0 = \delta \sum_{i=1}^{p-1} \chi(i) = \sum_{i=1}^{p-1} (A_i - A_0) = \sum_{i=0}^{p-1} A_i - pA_0,$$

we find that $|\sum_{i=0}^{p-1} A_i| = p|A_0| = p$. On the other hand, $|\sum_{i=0}^{p-1} A_i| \leq \sum_{x=1}^{p-1} |f_2(x)| = p-1$. Thus $A_0 = 0$, and it follows that $A_i = \delta\chi(i)$ for $i \neq 0$. In other words, $a_{p^{k-1}j} = A_j = \delta\chi(j)$ for $j = 1, 2, \ldots, p-1$,

and since there are at most $p-1$ nonzero values among the a_i's, the remaining ones must all be equal to zero. $\square$

Now, the lemma gives that $\zeta_{p^k}^s f_1(1)\psi(1) = \zeta_{p^k}^s \zeta_p$ is a p-th root of unity, hence p^{k-1} must divide s, and the nonzero values of $f_1(x)\psi(x)$ are thus distinct p-th roots of unity. Replacing ψ by ψ_r, for $r \not\equiv 0 \mod p$, in the previous argument gives that $f_1(x)\psi(rx)$ also ranges over distinct p-th roots of unity. On the other hand, if $f_1(x)$ is not constant, then there exists $r \not\equiv 0 \mod p$ such that the set $\{f_1(x)\psi_r(x)\}_{x=1}^{p-1}$ contains strictly less than $p-1$ elements. (If $f_1(x_1) \neq f_1(x_2)$, write $f_1(x_1) = \zeta_p^{y_1}$, $f_1(x_2) = \zeta_p^{y_2}$ and take $r \equiv -(y_2 - y_1)(x_2 - x_1)^{-1} \mod p$.) Hence $f_1(x)$ must be constant, and since $f_1(1) = 1$, we find that the nonzero values of $f(x)$ are in fact n-th roots of unity. The result has thus been reduced to the case $(m,p) = 1$.

References

1. A. Biro, *Notes on a problem of H. Cohn*, J. of Number Theory **77** (1999), no. 2, 200–208.
2. K.K.S Choi and M.K. Siu *Counter-Examples to a Problem of Cohn on Classifying Characters*, to appear in J. of Number Theory.
3. H. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, American Mathematical Society, Providence, RI, 1994.

Department of Mathematics, University of Georgia, Athens GA 30602 (`kurlberg@math.uga.edu`)